National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

EXTREMIST USE OF SOCIAL MEDIA - A NATIONAL SECURITY THREAT

Maj Katherine ME Krenn

JCSP 43 DL	PCEMI 43 AD
Exercise *Solo Flight*	**Exercice *Solo Flight***
Disclaimer	**Avertissement**
Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.	Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.
© Her Majesty the Queen in Right of Canada, as represented by the Minister of National Defence, 2018.	© Sa Majesté la Reine du Chef du Canada, représentée par le ministre de la Défense nationale, 2018.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES
JCSP 43 DL – PCEMI 43 AD
2017 – 2018

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

EXTREMIST USE OF SOCIAL MEDIA - A NATIONAL SECURITY THREAT

Maj Katherine ME Krenn

"This paper was written by a student attending the Canadian Forces College in fulfilment of one of the requirements of the Course of Studies. The paper is a scholastic document, and thus contains facts and opinions, which the author alone considered appropriate and correct for the subject. It does not necessarily reflect the policy or the opinion of any agency, including the Government of Canada and the Canadian Department of National Defence. This paper may not be released, quoted or copied, except with the express permission of the Canadian Department of National Defence."

Word Count: 3317

"La présente étude a été rédigée par un stagiaire du Collège des Forces canadiennes pour satisfaire à l'une des exigences du cours. L'étude est un document qui se rapporte au cours et contient donc des faits et des opinions que seul l'auteur considère appropriés et convenables au sujet. Elle ne reflète pas nécessairement la politique ou l'opinion d'un organisme quelconque, y compris le gouvernement du Canada et le ministère de la Défense nationale du Canada. Il est défendu de diffuser, de citer ou de reproduire cette étude sans la permission expresse du ministère de la Défense nationale."

Compte de mots: 3317

EXTREMIST USE OF SOCIAL MEDIA - A NATIONAL SECURITY THREAT

INTRODUCTION

In a globalized world that is more interconnected than ever before, social media plays a big role in terms of both challenges as well as opportunities for government and law enforcement agencies [Pandalai, 2016]. The ability for criminal and terrorist organizations to operate in the open poses a huge threat to global security, as laws to address the cyber domain struggle to keep up with the rapid pace of social media technology to address this growing problem. Social media continues to be a means to both promote their ideology as well as to recruit new followers [PSC, 2017]. As well, privacy concerns are also on the rise and must be met with a balanced government approach, otherwise this could lead to an increased fear of government/state censorship of the internet.

The purpose of this paper is to demonstrate the threat posed to national security by social media and to highlight the need to grant government authority for greater oversight of the internet. Analysis will focus on the term radicalization and how violent extremist organizations employ social media and encrypted applications and whether granting government authority for more oversight of the internet is a feasible solution to this growing threat. Analysis will commence with the drivers for radicalization followed by an examination of different extremist organizations' use of social media and encrypted applications. It will conclude with the recommendation for a conceptual security framework that incorporates a comprehensive, multi-agency, whole of government (WoG) approach, and a way forward for government and law enforcement agencies to partner with industry to combat this global threat [PSC, 2017].

DISCUSSION - RADICALIZATION

Since the New York City attacks of 9/11, government agencies have started to work closer together to address the threat of terrorism posed by violent extremist organizations. Post 9/11, radicalization was a term coined by European law enforcement and intelligence agencies that by definition meant "anger" [Coosaet, 10, 2014]. In 2004, the term radicalization became the foundation for an "internal European Union (EU) counterterrorism document that listed potential root causes for the "anger" [Coosaet, 10, 2014]. It is important to understand the history of how the term radicalization became accepted into mainstream, and how due to the "lack of consensus on the drivers that turn extremism into terrorism" assisted terrorist organizations to recruit more European youth to fight in overseas conflicts [Coolsaet, 10, 2014].

With a growing number of social media users, there is a new "bottom-up" vice "top-down" dynamic of small self-radicalizing groups and individuals that has developed" whereby "recruitment has become a more spontaneous local process, evolving through kinship and friendship bonds" [Coolsaet, 8, 2014]. Some drivers of radicalization for individuals could be religious in nature, while for others it could be due to economic or political reasons; there is no one set driver for radicalization. Then there are those who are attracted and adhere to "such ideologies and engage in terrorism-related activities, including participation in online extremist forums, circulation of extremist propaganda, terrorist financing, travelling to join terrorist groups abroad, and in some cases, planning and carrying out attacks" [PSC, 2017]. There are many different facets to radicalization and how an individual or group reacts to such drivers.

Social media and encrypted applications have "emerged as significant tools for violent extremists to enable and inspire attacks in the West" [PSC, 2017]. Despite the efforts from some social media companies to shut down social media accounts of both terrorist groups as well as sympathizers, both groups and individuals respond quickly by opening new accounts "to continue the spread of terrorist ideology" [PSC, 2017]. "Encryption technologies to the social media platforms has created channels of radicalization, recruitment, and activation over live chats and messages that cannot be indicted by authorities easily" [Terban, 2018].

When Al Qaeda (AQ) lost physical terrain to operate, social media "set the conditions for movement toward inciting the "far war" over the local struggle" through the use of their online magazine Inspire [Terban, 2018]. This Modus Operandi (MO) was cited as "Open Source Jihad" in the extremist group Daesh's magazine, Dabiq [Terban, 2018]. The investment of a nominal amount of money and energy has proven to pay large dividends to these groups, who are turning Social Media into the "bedrock of the fight against the West" [Terban, 2018]. Evidence of this can be seen in the number of what is being termed "Lone Wolf Jihad" throughout the West, with incidents such as those in New York City and Munster whereby civilians were killed by a lone driver in vehicle attack. In the case of New York, the driver was a green card holder to the U.S. from Uzbekistan, but the attacker in Munster "was not suspected of a political or organized terror-related motive" [Telegraph, 2018]. Although not all motives are clear, the link that they all have is that terrorist messaging is reaching a large audience, one that goes well beyond that of sympathizer to a cause, and is instilling a methodology of how to carry out an attack to create mass casualties. Even though not every event was motivated by a particular terrorist organization, extremist organizations can still indirectly take credit for these attacks, as they were studied and carried out using this particular MO [Terban, 2018].

Far-right groups, such as the U.S. based Three Percenters, utilize social media to attract others to their cause, and over the past few years have emerged in various parts of Canada [Hutter, 2018]. One expert at the Centre for the Prevention of Radicalization Leading to Violence believes that this is the most dangers group in Canada right now, as it continues to increase their ability to fight back [Hutter, 2018]. Despite this assessment, a "spokesperson for the RCMP said the force does not investigate movements or ideologies but will investigate the criminal activity of any individuals who threaten the safety and security of Canadians" [Hutter, 2018]. This group could be viewed as "a far-right prepper militia movement that is actively arming and engaging in paramilitary training" and with the RCMP unable or unwilling to investigate this movement, they are free to operate in the open and use social media to recruit, train, and conduct operations [Hutter, 2018]. In this particular scenario, the group was formed by like-minded individuals who are "armed and ready to defend themselves against the government, should it turn tyrannical" [Hutter, 2018]. A knock on effect to this belief is that should law enforcement act upon information that this group is involved in illegal activity, they would feel legitimized. Conversely, should law enforcement do nothing, citing no criminal activity is/has occurred, the group will continue to grow and train its membership and spread its ideology.

In 2016, the Baqiya family, "which is a loose global network of Daesh supporters, significantly expanded its online presence"… "to brainstorm attack methodologies, share operational information, inspire attacks against the West, and to build a sense of community among extremists" [PSC, 2017]. Twitter and Facebook are the two main social media platforms, with "Twitter being the epicentre" and often referred to as "Jihadi Twitter" [Miller, 2015]. "You can be in direct communication with a fighter in Syria within about 15 seconds. That's part of the appeal, a lot of these youths feel like they're part of something greater than themselves" [Miller, 2015]. The Baqiya online network can accelerate the development and radicalization of a "troubled youth into an active terrorist" in the "search for purpose and the promise of more" [Bain, 3, 2016]. "Radicalization is to an underlying factor what fever is to illness – a symptom.

Sometimes, medicine against fever will alleviate the suffering, but as a term should be viewed the same as a fever is to illness – a symptom" [Coosaet, 46, 2016].

The two aforementioned extremist organizations were used as examples to highlight the use of social media by both Muslim and anti-Muslim groups to spread their ideology. Despite their differing views of hatred, the one thing they have in common is their ability to use the internet to their advantage. In Canada, one Liberal MP "tabled a motion calling on the government to condemn Islamophobia and develop a strategy to combat it" [Harris, 2017]. The motion of M-103 was aimed to "condemn and combat Islamophobia, acts of discrimination and hate against Muslims" [Harris, 2017]. Although this motion may have seemed like a good idea at its conception, there was a risk that it "could infringe on free speech and the charter right to freedom of expression, because criticism of Islam could be construed as Islamophobia" [Harris, 2017]. Using this logic, and the two groups above, this would also run the risk of generating more sympathizers for far-right organizations and it would also legitimize Muslim extremist messaging that there is a Western hatred toward Islam; not a win-win situation.

DISCUSSION - GOVERNMENT OVERSIGHT

Until recently, the US government has oversight of the Internet with vested authority from "The Domain Openness Through Continued Oversight Matters (DOTCOM) Act that required the Government Accountability Office to review any proposal to cede current U.S. Internet oversight responsibilities to a group of international stakeholders" [Shimkus, 2014]. The Internet Corporation for Assigned Names and Numbers (ICANN), a California based non-profit organization, was created in 1998 " to ensure the Internet would never be controlled by governments or an intergovernmental organization like the United Nations (UN)" [Shimkus, 2016]. Further rationale for this organization is that it denied hostile countries such as Russia and China the ability to manipulate the internet for their own nationalistic purposes as they had previously attempted to do with the United Nation's International Telecommunication Union (ITU) [Shimkus, 2014]. "U.S. government oversight was never intended to be a permanent feature of the internet governance, but rather a temporary measure to be removed once ICANN could operate independent of government control" [Shimkus, 2016]. This transition is a powerful step "and an affirmation of the principle that the best approach to address challenges is through bottom-up, transparent, and consensus-driven processes" [AFP, 2016]. The transition came with one exception, and that was for the U.S. General Services Administration (GSA) to be delegated control of the ".gov" suffix and that it be restricted for use by government agencies in the U.S. [AFP, 2016].

This shift to a privatized governance structure is cited by many throughout the international arena as a positive step, but it disconnects the U.S. federal government from the issue to "legislate data security practices" as laws and regulations continue to move slower than that of technology and business practices [Duncan, 2014]. Further, with a lack of U.S. government oversight, violent extremist organizations may have the ability to operate more freely and without reprisal thereby creating a potential impact to government sponsored counterterrorism efforts.

"Counterterrorism should be a whole-of-government effort, encompassing complex societal issues such as integration, multiculturalism and social cohesion, and stitching it all together in a broadened security agenda" [Coosaet, 10, 2014]. Therefore, should the solution be for government agencies to partner with social media companies to share information, there must be some level of government oversight and control in order to help effect this change.

Extremist organizations will continue to use social media to spread their ideology; it is part of the current national and global security threat and is something that will never go away. Empowering law enforcement agencies to deal with this threat, to monitor and police the internet will be critical to developing a successful, holistic response [Terban, 2018]. One of the outstanding challenges facing the idea of government oversight and partnership with social media companies is the "legal interpretation concerning the balance of what constitutes freedom of speech and what constitutes illegal activity" [Terban, 2018]. Further, government oversight is only scratching the surface of the problem; an effective online counter-message to neutralize extremist messaging also needs to be developed and agencies at all levels of government and industry need to be involved [Bokhari, 2016]. Conversely, it should be the smaller, grass-roots agencies that lead the effort as they are close to the community and are not perceived to bear any government affiliation [Toor, 2016]. In 2015, when Facebook and Google conducted an experiment to determine if messaging was being received by their target audience, they determined that in fact it was. However, the second part of the experiment, to determine whether there was any success with online de-radicalization could not be proven [Toor, 2016]. This is a good metric to work with because a counter-message is only good if it is received by the target audience. Coupled with counter-messaging, other recommendations to address this problem include: "community-level engagement, that incorporates a campaign to address extremist discourses and the presence of recruiters in communities; tailoring the message to the audience; restrictive measures – website takedowns and content filtering paired with counter-messaging; provide causal alternatives to false extremist narratives; affirm correct information rather than negate incorrect beliefs" [Goldfien, 2015]. The problem of extremist organizations using social media to conduct their activities may never be completely eradicated, but authorizing government greater oversight and control in conjunction with the aforementioned recommendations may be the most plausible answer that government has at this time to combat the threat.

CONCLUSION

The world has become smaller today than ever before, due in large part to the number of subscribers to social media. The ability for criminal and terrorist organizations to operate in the open is a huge threat to global security, and technology has outpaced government capacity to create new law to address the cyber domain. Social media and encrypted applications have "emerged as significant tools for violent extremists to enable and inspire attacks in the West" [PSC, 2017]. As quickly as a social media company shuts down accounts of both terrorist groups as well as sympathizers, both groups and individuals respond quickly by opening new accounts "to continue the spread of terrorist ideology" [PSC, 2017]. "Encryption technologies to the social media platforms has created channels of radicalization, recruitment, and activation over live chats and messages that cannot be indicted by authorities easily" [Terban, 2018].

Concerns over privacy and the protection of online information are also on the rise, and populations are looking to government to implement stronger legislation to protect private citizens. But this level of oversight and control must be met with a balanced government approach; otherwise this could lead to an increased fear of government/state censorship of the internet.

Due to the threat posed from extremist use of social media to national security, greater government oversight and control of the internet should be established. Government partnership with industry and social media companies is necessary to build required databases of individuals and/or groups suspected of illegal activity online. As previously highlighted, these partnerships would have to be developed carefully between public and private institutions as it could otherwise have the potential to lead to legal privacy issues and the level of government jurisdiction. As the number of social media users continues to increase at an exponential rate, the new dynamic of a bottom-up vice top-down dynamic of small self-radicalizing groups and individuals must be addressed. Law enforcement agencies should be empowered to conduct community-level engagements as part of a counter-messaging campaign [Goldfien, 2018]. It is also equally important to understand the history of the term "radicalization" and to understand that there are many drivers to this term; that it is not a catchall phrase for all organizations. Failure to understand this basic principle could work to the benefit of an extremist organization, as history has proven [Coolsaet, 10, 2014].

Ultimately what is required is a conceptual security framework that incorporates a comprehensive, multi-agency, whole of government (WoG) approach, and a way forward for government and law enforcement agencies to partner with industry to combat this global threat. [PSC, 2017]. It must take into account human interaction and the need for community level engagement, as a technological solution alone would be ineffective. The need to understand how to reach out to a community online is also a critical component to a successful outcome. As the 2015 experiments conducted by Facebook and Google concluded, although information may be "viral" it may or may not have been received by the target audience [Toor, 2016]. This metric can now be used to gauge the success of other counter-messaging campaigns as part of a cyclical analytic process.

BIBILIOGRAPHY

AFP: *US government gives up formal oversight over the internet and hands management of the web's address book to a non-profit.* October 1, 2016. http://www.dailymail.co.uk/news/article-3817113/US-cuts-cord-internet-oversight.html

Bain, Alexandra: *Talking to Foreign Fighters. Socio-Economic Pus versus Existential Pull Factors. Canadian Network for Research on* Terrorism, Security and Society (TSAS) - Working Paper Series. No 16-14. July 2016. Accessed online May 2, 2018. https://www.globalgovernancewatch.org/library/doclib/20160831_TalkingtoForeignFighters.pdf

Bokhari, Kamran: *Extremism and Counter-Messaging.* Reality Check, Geopolitical Futures. March 21, 2017. https://geopoliticalfutures.com

Coolsaet, Rik: *All Radicalisation is Local- The genesis and drawbacks of an elusive concept.* Egmont, Royal Institute for International Relations. Egmont Paper 84 June 2016. http://www.academia.edu/25860940/all_radicalisation_is_local_the_genesis_and_drawbacks_of_an_elusive_concept

Duncan, Geoff: *Can the government regulate Internet privacy?* April 21, 2014. Digital Trends. Accessed online May 8 2018. https://www.digitaltrends.com/web/government-warn-us-data-breaches/

Goldfien, Michael: *Countering Extremist Speech Online- A Report tot eh Bureau of Conflict & Stabilization Operations U.S. Department of State.* Stanford University. June 2015. https://www-cdn.law.stanford.edu/wp-content/uploads/2016/07/Goldfien-and-Woolslayer-Countering-Extremist-Speech-Online-A-Report-to-the-Department-of-State.pdf

Harris, Kathleen: *5 things to know about the Commons motion on Islamophobia.* February 17, 2017. CBC News. http://www.cbc.ca/news/politics/iqra-khalid-islamophobia-motion-1.3987668

Hutter, Kristy: *Three Percenters are Canada's "most dangerous" extremist group, say some experts.* May 10, 2018. CBC News. http://www.cbc.ca/news/canada/three-percenters-canada-1.4647199

Miller, Nick: *Global terror `family`Baqyia a growing concern for security.* The Sydney Morning Herald. October 3, 2015. https://www.smh.com.au/world/global-terror-family-baqiya-a-growing-concern-for-security-20151003-gk0fq5.html Amarnath Amarasingam

Pandalai, Shruti: *The Social Media Challenge to National Security: Impact and Opportunities- A Conceptual Overview.* Monograph No. 55, 2016. Institute for Defence Studies and Analyses. Accessed online May 2, 2018. https://idsa.in/monograph/social-media-challenge-to-national-security

Public Safety Canada: *2017 Public Report on the Terrorist Threat to Canada.* December 21, 2017. Accessed online May 2 2018. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/pblc-rprt-trrrst-thrt-cnd-2017/index-en.aspx

Shimkus, John: *Shimkus Seeks Review of Proposal to Relinquish Longstanding U.S. Internet Oversight Role*. September 30, 2016. Press Release. https://shimkus.house.gov/media-center/opeds/department-of-commerce-to-end-oversight-of-internet-domain-name-system

Shimkus, John: *Department of Commerce to End Oversight of Internet Domain Name System.* December 9, 2017. Press Release. https://shimkus.house.gov/media-center/opeds/department-of-commerce-to-end-oversight-of-internet-domain-name-system

Telegraph Reporters: *Timeline of vehicle rampage attacks in Europe.* April 9, 2018. https://www.telegraph.co.uk/cars/news/timeline-vehicle-terror-attacks-europe/

Terban, Scot: *An Assessment of Violent Extremist Use of Social Media Technologies.* Real Clear Defense Online Magazine. February 5, 2018. https://www.realcleardefense.com/articles/2018/02/05/an_assessment_of_violent_extremist_use_of_social_media_technologies_113015.html

Toor, Amar: *Facebook, Google, and Twitter combat online extremism with targeted videos.* The Verge online. August 4, 2016. https://www.theverge.com/2016/8/4/12373978/facebook-google-twitter-extremism-counter-speech-isd-isis